REMARKS

Applicant respectfully requests consideration and allowance of the pending claims. Claims 1, 11 and 23 are independent. Claim 31 is amended to rectify a minor informality thereof. Applicant thanks the Examiner for the detailed analysis presented in the Office Action of April 5, 2007.

Implementation Introduction

Before discussing the rejections of the current Office Action, the Applicant provides the following discussion of at least one implementation described in the instant Application. The following discussion does not limit the claims pending in the Application.

One implementation of the Application may be used in conjunction with a computing device that implements a resource–sparing operating system. Windows CE is an example of a resource–sparing operating system. Those of ordinary skill in the art understand that resource–sparing operating systems are often implemented in computing devices that have limited storage and memory resources. In one implementation described in the instant Application, a resource–sparing operating system is implemented in a flash memory of a computing device. Embodiments described in the Application help to ensure that a correct resource–sparing operating system is booted by a computing device.

One implementation of the instant Application includes a resource–sparing operating system image that includes a catalog file embedded therein. As those of ordinary skill in the art readily understand, a "catalog file" is a binary file that lists the state of all the settings and packages in an image file. When a catalog is created, it queries the image for a list of all the settings in that image. Because the

contents of the image can change over time, it may be important to recreate the catalog file whenever the image is updated. A hash is created from the resource–sparing operating system image. As those of ordinary skill in the art understand, a hash is a digital "fingerprint" of the data. An algorithm "chops and mixes" (i.e., substitutes or transposes) the data to create such fingerprints. Another hash of the resource–sparing operating system image is created from the catalog file. The use of the resource–sparing operating system image is blocked if the two hashes do not match.

Claim Rejections Under § 102

Claims 23-34 stand rejected as being unpatentable under 35 U.S.C. § 102(e) in view of U.S. Patent No. 6,684,326 to Cromer et al. ("Cromer"). Applicant respectfully traverses this rejection.

Applicant addresses the rejection of the independent claims in the following. As a preliminary matter, Applicant does not separately address the patentability of each remaining dependent claim in detail. However, Applicant's decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that Applicant concurs with the Office's conclusion that these dependent claims are not patentable over the disclosure in the cited references. Similarly, Applicant's decision not to discuss differences between the prior art and every claim element, or every comment made by the Office, should not be considered as an admission that Applicant concurs with the Office's interpretation and assertions regarding those claims. Indeed, Applicant believes that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each

dependent claim is not required, since dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims ultimately depend.

Claim 23 recites:

> A portable computing device, comprising:
> flash memory, the flash memory including *a protected area and an unprotected area*;
> a *bootloader stored in the protected area* of flash memory, the bootloader containing a crypto module;
> an *operating system image stored in the unprotected area* of flash memory;
> random access memory (RAM); and
> wherein the crypto module of the *bootloader is operative to examine an image update* to determine if the image update should be programmed into the unprotected area of flash memory to boot the device *based on information included in a signed catalog file embedded* in the image update. (Emphasis added.)

Applicant respectfully submits that the relied upon patent neither discloses nor suggests what is recited by independent claim 23 for at least the following reasons.

The Cromer patent describes methods and systems for performing an authenticated boot of a computer system in a networked computing environment. Cromer discusses the authenticated process in *column 5, lines 15 – 63,* of the relied upon patent.

According to Cromer, a client system 104 is first powered on. Then, a boot BIOS reviews a boot device list to determine and select a bootable hardware element that includes an operating system. Cromer does not disclose or suggest that the boot BIOS is stored in a "protected area of flash memory." (Claim 23.) Moreover, Cromer does not disclose or suggest that the operating system is stored in an "unprotected area of flash memory." (Claim 23.)

The Office states that flash memory is disclosed in the Cromer patent at *column 4, lines 17 – 57.* The indicated section of the patent discloses a protected storage 262. However, there is nothing that discloses or suggests that the protected storage 262 is used for anything other than the storage of master keys. (*See column 4, lines 38 – 39.*) And Cromer is completely silent regarding the storage of an operating system in an "unprotected area of flash memory."

According to the process described in the Cromer patent, once a bootable operating system image is found by the boot BIOS, an encryption chip 261 signs the boot record associated with the operating system image. (*See column 5, lines 34 – 38.*) The boot BIOS then hashes the boot record, encrypts the hash, and sends the signed hash to a server 100. (*See column 5, lines 37 – 41.*) The server 100 determines if the boot record is valid. Therefore, the process according to the Cromer patent does not disclose or suggest "the *crypto module of the bootloader* is operative to *examine an image update* to determine if the image update should be programmed into the unprotected area of flash memory to boot the device based on information included in *a signed catalog file embedded in the image update.*" (Emphasis added.) More specifically, the boot BIOS of the Cromer performs an encryption process, but fails to *examine an image* of the operating system. Therefore, it is impossible that the boot BIOS is capable of determining "if the image update should be programmed into the unprotected area of flash memory to boot the device based on information included in *a signed catalog file embedded in the image update.*"

In accordance with the above, Applicant submits that Cromer neither discloses nor suggests the recitation of claim 23. Thus, claim 23 is patentable over the cited reference. Furthermore, because claims 24 – 34 are patentable for at least the same reasons as the independent claim from which they depend, and because they add additional features to claim 23, Applicant submits that claims 24 – 34 also are patentable. Accordingly, Applicant respectfully requests that the rejection under 35 U.S.C. § 102(e) be withdrawn against the pending claims.

Claim Rejections Under § 103

Claims 1-22 stand rejected as being unpatentable under 35 U.S.C. § 103(a) in view of U.S. Patent No. 5,781,773 to Vanderpool et al. ("Vanderpool") in view of Cromer. Applicant respectfully traverses this rejection.

Claim 1 recites:

> A method of file system protection for *a resource-sparing operating system (OS) image*, comprising the steps of:
> loading *the image* into random access memory (RAM), the image including a catalog file embedded therein;
> creating *a first hash of the image*;
> extracting *a second hash of the image from the catalog file*; and
> *blocking the use of the image to boot the computing device when the first hash and the second hash do not match.* (Emphasis added.)

Respectfully, none of the references, alone or in combination, discloses or suggests what is recited by claims 1 and 11 for at least the following reasons.

The Vanderpool patent discloses a method of transforming and storing data for search and display by a computer system. The relied upon patent discusses the compression of image data and alignment of such image data with related summary data. (*See Abstract.*)

The Office maintains that the Vanderpool patent discloses an "image including a *catalog file embedded therein*." (Claim 1.) It is asserted that *column 11, lines 31–35* of the Vanderpool patent discloses the foregoing subject matter. The Applicant disagrees with the Office's assessment of Vanderpool.

The patent discloses that a compressed thumbnail image 48 may be loaded into random access memory 126. Summary data fields 158 may also be loaded into the memory 126. (*See column 11, lines 31 – 41.*) The images 48 are *not* resource–sparing operating system images. This is clearly seen in figure 11 of the Vanderpool patent. Instead, Vanderpool discloses that the compressed images are in standard *JPEG* format. Those of ordinary skill in the art readily understand that JPEG formatted images are not remotely related to operating system images. (*See column 11, lines 63 – 65.*) Certainly, such JPEG formatted images do not include "a catalog file embedded therein." (Claim 1.)

Vanderpool also does not disclose or suggest "creating *a first hash* of the image; [and] extracting *a second hash of the image from the catalog file*." (Claim 1.) The patent does disclose the use of a hash algorithm to *copy* compressed images and text supplements 18 to about 100 subdirectories. (*See column 7, lines 61 – 64.*) In particular, Vanderpool discloses that the hash algorithm may be any hash algorithm which places the images and text supplements in the 100 subdirectories. (*See column 8, lines 5 – 8.*) Although the hash algorithm used by Vanderpool does copy compressed images to a particular location, the used hash algorithm does not *create* a hash of the compressed images.

The Office maintains that the "catalog file" recited in claim 1 may be broadly interpreted as a data "linked" to a compressed image. (*Current Office Action, page 6, last paragraph.*) Applicant respectfully submits that "linked" is

not a synonym of "embedded." Moreover, even a brief review of figure 11 of the Vanderpool patent shows that the text supplements are not *embedded* in the images 48.

The Office acknowledges that Vanderpool fails to disclose or suggest "blocking the use of the image to boot the computing device when the first hash and the second hash do not match." (Claim 1.) The Office looks to Cromer to remedy this particular deficiency of Vanderpool. However, even if Cromer were to disclose or suggest the indicated limitation of claim 1, which the Applicant does not admit, the Cromer patent does not remedy the deficiencies of Vanderpool discussed hereinabove.

Accordingly, Applicant respectfully submits that the combination of Vanderpool in view of Cromer neither discloses nor suggests the limitations of claim 1. Similarly, the combination of Vanderpool in view of Cromer fails to disclose or suggest what is recited in claim 11. In particular, the combination fails to disclose or suggest at least "a resource-sparing operating system (OS) image, the image including a catalog file embedded therein,… examining the catalog file and the image to determine if the image is a properly released image; and blocking use of the image to boot the computing device when the step of examining determines that the image is not a properly released image." (Claim 11.) Claims 2-10 and 12-22 are at least allowable due to their dependency upon an allowable independent claim, as well as for additional limitations set forth by the claims.

The detailed discussion above shows that Vanderpool and Cromer, whether taken alone or in combination together, fail to disclose or suggest the claims rejected under 35 U.S.C. § 103(a). Accordingly, reconsideration and withdrawal of the rejection are respectfully requested.

Conclusion

In accordance with the foregoing remarks, Applicant believes that the pending claims are allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the Applicant at the telephone number provided below.

Respectfully Submitted,

Dated: July 3, 2007

By: / Lewis C Lee Reg No 34656 /
Lewis C. Lee
Reg. No. 34,656
(509) 324-9256